Le chiffrement, maintenant (2)

Voici la deuxième partie du guide sur le chiffrement que nous vous avons présenté la semaine dernière.

Ces derniers jours, les révélations distillées par Snowden n'ont fait que confirmer l'ampleur considérable des transgressions commises par la NSA : le protocole https est compromis, et même un certain type de chiffrement a été « cassé » depuis 2010…

Il est donc d'autant plus justifié de rechercher les moyens de se protéger de ces intrusions de la surveillance généralisée dans nos données personnelles. À titre d'introduction à notre chapitre de la semaine, j'ai traduit rapidement 5 conseils donnés ce vendredi par Bruce Schneier, spécialiste de la sécurité informatique, dans un article du Guardian. Il reconnaît cependant que suivre ces conseils n'est pas à la portée de l'usager moyen d'Internet…

> *1) **Cachez-vous dans le réseau.** Mettez en œuvre des services cachés. Utilisez Tor pour vous rendre anonyme. Oui, la NSA cible les utilisateurs de Tor, mais c'est un gros boulot pour eux. Moins vous êtes en évidence, plus vous êtes en sécurité.*
>
> *2) **Chiffrez vos communications.** Utilisez TLS. Utilisez IPsec. Là encore, même s'il est vrai que la NSA cible les connexions chiffrées – et il peut y avoir des exploits explicites contre ces protocoles – vous êtes beaucoup mieux protégés que si vous communiquez en clair.*
>
> *3) **Considérez que bien que votre ordinateur puisse être compromis, cela demandera à la NSA beaucoup de travail et de prendre des risques – il ne le sera donc probablement pas.** Si vous avez quelque chose de vraiment important entre les mains, utilisez un « angle mort ». Depuis que j'ai commencé à*

travailler avec les documents Snowden, j'ai acheté un nouvel ordinateur qui n'a jamais été connecté à l'internet. Si je veux transférer un fichier, je le chiffre sur l'ordinateur sécurisé (hors-connexion) et le transfère à mon ordinateur connecté à Internet, en utilisant une clé USB. Pour déchiffrer quelque chose, j'utilise le processus inverse. Cela pourrait ne pas être à toute épreuve, mais c'est déjà très bien.

4) ***Méfiez-vous des logiciels de chiffrement commerciaux, en particulier venant de grandes entreprises.*** *Mon hypothèse est que la plupart des produits de chiffrement de grandes sociétés nord-américaines ont des portes dérobées utiles à la NSA, et de nombreuses entreprises étrangères en installent sans doute autant. On peut raisonnablement supposer que leurs logiciels ont également ce genre de portes dérobées. Les logiciels dont le code source est fermé sont plus faciles à pénétrer par la NSA que les logiciels open source. Les systèmes qui reposent sur une clé « secrète » principale sont vulnérables à la NSA, soit par des moyens juridiques soit de façon plus clandestine.*

5) ***Efforcez-vous d'utiliser un chiffrement du domaine public qui devra être compatible avec d'autres implémentations.*** *Par exemple, il est plus difficile pour la NSA de pénétrer les TLS que BitLocker, parce que les TLS de n'importe quel fournisseur doivent être compatibles avec les TLS de tout autre fournisseur, alors que BitLocker ne doit être compatible qu'avec lui-même, donnant à la NSA beaucoup plus de liberté pour le modifier à son gré. Et comme BitLocker est propriétaire, il est beaucoup moins probable que ces changements seront découverts. Préférez le chiffrement symétrique au chiffrement à clé publique. Préférez les systèmes basés sur un logarithme discret aux systèmes conventionnels à courbe elliptique ; ces derniers ont des constantes que la NSA influence quand elle le peut.*

Type de menace

D’après Encryption Works

(contributeurs : audionuma, goofy, lamessen, Calou, Achille Talon)

La NSA est un puissant adversaire. Si vous êtes sa cible directe, il vous faudra beaucoup d’efforts pour communiquer en toute confidentialité, et même si ce n’est pas le cas, des milliards d’innocents internautes se retrouvent dans les filets de la NSA.

Bien que les outils et conseils présentés dans ce document soient destinés à protéger votre vie privée des méthodes de collecte de la NSA, ces mêmes conseils peuvent être utilisés pour améliorer la sécurité de votre ordinateur contre n’importe quel adversaire. Il est important de garder à l’esprit que d’autres gouvernements, notamment la Chine et la Russie, dépensent d’énormes sommes pour leurs équipements de surveillance et sont réputés pour cibler spécifiquement les journalistes et leurs sources. Aux États-Unis, une mauvaise sécurité informatique peut coûter leur liberté aux lanceurs d’alerte, mais dans d’autres pays c’est leur vie même que risquent à la fois les journalistes et leurs sources. Un exemple récent en Syrie a montré à quel point une mauvaise sécurité informatique peut avoir des conséquences tragiques.

Mais la modification de certaines pratiques de base peut vous garantir une bonne vie privée, même si cela ne vous protège pas d’attaques ciblées par des gouvernements. Ce document passe en revue quelques méthodes qui peuvent vous servir dans les deux cas.

Systèmes de crypto

> *Nous avons découvert quelque chose. Notre seul espoir contre la domination totale. Un espoir que nous pourrions utiliser*

> *pour résister, avec courage, discernement et solidarité. Une étrange propriété de l'univers physique dans lequel nous vivons.*
>
> *L'univers croit au chiffrement.*
>
> *Il est plus facile de chiffrer l'information que de la déchiffrer.*

— Julian Assange, in Menace sur nos libertés : comment Internet nous espionne, comment résister

Le chiffrement est le processus qui consiste à prendre un message textuel et une clé générée au hasard, puis à faire des opérations mathématiques avec ces deux objets jusqu'à ce qu'il ne reste plus qu'une version brouillée du message sous forme de texte chiffré. Déchiffrer consiste à prendre le texte chiffré et sa clé et à faire des opérations mathématiques jusqu'à ce que le texte initial soit rétabli. Ce domaine s'appelle la cryptographie, ou crypto en abrégé. Un algorithme de chiffrement, les opérations mathématiques à réaliser et la façon de les faire, est un ensemble appelé « code de chiffrement ».

Pour chiffrer quelque chose vous avez besoin de la bonne clé, et vous en avez aussi besoin pour la déchiffrer. Si le logiciel de chiffrement est implémenté correctement, si l'algorithme est bon et si les clés sont sécurisées, la puissance de tous les ordinateurs de la Terre ne suffirait pas à casser ce chiffrement.

Nous développons des systèmes de cryptographie qui relèvent de problèmes mathématiques que nous imaginons difficiles, comme la difficulté à factoriser de grands nombres. À moins que des avancées mathématiques puissent rendre ces problèmes moins complexes, et que la NSA les garde cachées du reste du monde, casser la crypto qui dépend d'eux au niveau de la sécurité est impossible.

La conception des systèmes de chiffrement devrait être complètement publique. Le seul moyen de s'assurer que le code de chiffrement ne contient pas lui-même de failles est de publier son fonctionnement, pour avoir de nombreux yeux qui le scrutent en détail et de laisser les experts des véritables attaques à travers le monde trouver les bogues. Les mécanismes internes de la plupart des cryptos que nous utilisons quotidiennement, comme le HTTPS, cette technologie qui permet de taper son code de carte bancaire et les mots de passe sur des formulaires de sites internet en toute sécurité, sont totalement publics. Un attaquant qui connaît parfaitement chaque petit détail du fonctionnement du système de chiffrement ne réussira pas à le casser sans en avoir la clé. En revanche, on ne peut pas avoir confiance dans la sécurité d'une cryptographie propriétaire et dans son code sous-jacent.

Voici une question importante à se poser lors de l'évaluation de la sécurité d'un service ou d'une application qui utilise la crypto : est-il possible pour le service lui-même de contourner le chiffrement ? Si c'est le cas, ne faites pas confiance à la sécurité du service. Beaucoup de services comme Skype et Hushmail promettent un chiffrement « de bout en bout », mais dans la majorité des cas cela signifie aussi que les services eux-même ont les clés pour déchiffrer le produit. Le véritable chiffrement « de bout en bout » signifie que le fournisseur de service ne peut pas lui-même regarder vos communications, même s'il voulait le faire.

Un aspect important du chiffrement est qu'il permet bien plus que la protection de la confidentialité des communications. Il peut être utilisé pour « signer électroniquement » les messages d'une manière qui permette de prouver que l'auteur du message est bien celui qu'il prétend être. Il peut également être utilisé pour utiliser des monnaies numériques comme Bitcoin, et il peut être utilisé pour produire des réseaux qui permettent l'anonymat comme Tor.

Le chiffrement peut aussi servir à empêcher les gens

d’installer des applications pour iPhone qui ne proviennent pas de l’App Store, à les empêcher d’enregistrer des films directement à partir de Netflix ou encore les empêcher d’installer Linux sur une tablette fonctionnant sous Windows 8. Il peut aussi empêcher des attaques de type « homme du milieu » (NdT : attaque consistant à intercepter les communications entre deux terminaux sans que ces derniers se doutent que la sécurité est compromise) d’ajouter des malwares pour compromettre les mises à jour légitimes de logiciels.

En bref, le chiffrement englobe de nombreux usages. Mais ici nous nous contenterons de regarder comment nous pouvons l’utiliser pour communiquer de façon sécurisée et privée.

(à suivre…)